PCT/JP03/11706

12.09.03

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

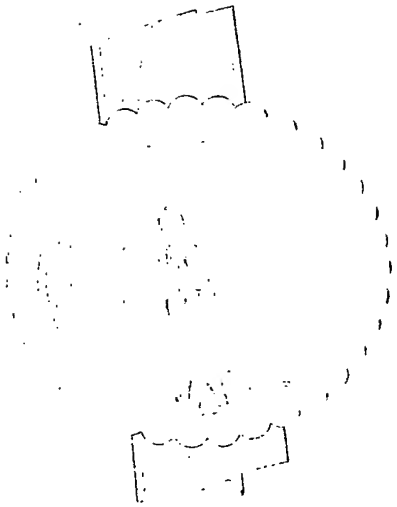
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　９月１８日

出願番号
Application Number: 特願２００２－２７１４７３

[ST. 10/C]: [ＪＰ２００２－２７１４７３]

出願人
Applicant(s): 三菱電機株式会社
理化学研究所

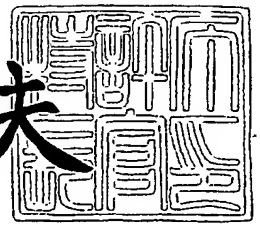


PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００３年１０月１７日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号　出証特２００３－３０８５５２１

【書類名】　特許願

【整理番号】　541636JP01

【提出日】　平成14年 9月18日

【あて先】　特許庁長官殿

【国際特許分類】　H03M 13/00

G09C　1/00　610

【発明者】

【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

【氏名】　松本　渉

【発明者】

【住所又は居所】　埼玉県和光市広沢２番１号　理化学研究所内

【氏名】　渡辺　曜大

【特許出願人】

【識別番号】　000006013

【氏名又は名称】　三菱電機株式会社

【特許出願人】

【識別番号】　000006792

【氏名又は名称】　理化学研究所

【代理人】

【識別番号】　100089118

【弁理士】

【氏名又は名称】　酒井　宏明

【手数料の表示】

【予納台帳番号】　036711

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【物件名】　委任状　1

【援用の表示】　手続補足書にて提出の委任状

【包括委任状番号】　9803092

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　量子鍵配送方法および通信装置

【特許請求の範囲】

【請求項１】　光子を量子通信路上に送信する第１の通信装置と当該光子を測定する第２の通信装置で構成された量子暗号システムにおける量子鍵配送方法において、

前記第１および第２の通信装置が、同一のパリティ検査行列Ｈ（ｎ×ｋ）を生成する検査行列生成ステップと、

前記第１の通信装置が、乱数列（送信データ）を発生し、さらに所定の送信コード（基底）をランダムに決定し、前記第２の通信装置が、所定の受信コード（基底）をランダムに決定する乱数発生ステップと、

前記第１の通信装置が、前記送信データと送信コードの組み合わせによって規定された量子状態で、光子を量子通信路上に送信する光子送信ステップと、

前記第２の通信装置が、量子通信路上の光子を測定し、前記受信コードと測定結果の組み合わせによって規定された受信データを得る光子受信ステップと、

前記第１および第２の通信装置が、前記測定が正しい測定器で行われたものかどうかを調べ、正しい測定器で測定されたｎビットの受信データおよび対応する送信データを残し、その他を捨てるデータ削除ステップと、

前記第１の通信装置が、前記パリティ検査行列Ｈとｎビットの送信データに基づくｋビットの誤り訂正情報を、公開通信路を介して前記第２の通信装置に通知する誤り訂正情報通知ステップと、

前記第２の通信装置が、前記パリティ検査行列Ｈとｎビットの受信データと誤り訂正情報に基づいて、受信データの誤りを訂正する誤り訂正ステップと、

前記第１および第２の通信装置が、公開された誤り訂正情報に応じて誤り訂正後の共有情報（ｎ）の一部（ｋ）を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を装置間の共有鍵とする暗号鍵生成ステップと、

を含むことを特徴とする量子鍵配送方法。

【請求項２】　前記検査行列生成ステップにあっては、

基本行列として有限アフィン幾何を用い、ガウス近似法による最適化を行うこ

とによって、パリティ検査行列の最適な行と列の重み配分を探索する重み探索ステップと、

前記最適な重み配分に基づいて、前記有限アフィン幾何の行および列の重みを所定の手順でランダムに分割し、列と行の重みまたはどちらか一方が均一でない低密度パリティ検査符号のパリティ検査行列Ｈを生成する分割ステップと、

を含むことを特徴とする請求項１に記載の量子鍵配送方法。

【請求項３】　前記検査行列生成ステップにあっては、さらに、「ＨＧ＝０」を満たす生成行列Ｇ（（ｎ－ｋ）×ｎ）から、$G^{-1}\cdot G=I$（単位行列）となる逆行列G^{-1}（ｎ×（ｎ－ｋ））を生成し、

前記暗号鍵生成ステップにあっては、逆行列G^{-1}を用いて共有情報（ｎ）の一部（ｋ）を捨てることを特徴とする請求項１または２に記載の量子鍵配送方法。

【請求項４】　前記検査行列生成ステップにあっては、さらに、ｎ次元ベクトルをｍ（$m\leqq n-k$）次元ベクトルに写す写像Ｆで、任意のｍ次元ベクトルｖに対して、写像Ｆと「ＨＧ＝０」を満たす生成行列Ｇの合成写像Ｆ・Ｇにおける逆像$(F\cdot G)^{-1}$（ｖ）の元の個数がｖによらず一定（2^{n-k-m}）であるものを生成し、

前記暗号鍵生成ステップにあっては、写像Ｆを用いて共有情報（ｎ）の一部を捨てることを特徴とする請求項１または２に記載の量子鍵配送方法。

【請求項５】　前記暗号鍵生成ステップにあっては、前記パリティ検査行列Ｈの列に対してランダム置換を実行し、前記パリティ検査行列Ｈの生成元の有限アフィン幾何ＡＧ（２，2^s）の１列目の中から特定の「１」を選び、その位置を、公開通信路を介して交換し、前記置換後のパリティ検査行列から前記「１」に対応する分割後の位置（列）、および巡回シフトされた各列における前記「１」に対応する分割後の位置（列）、を特定し、その特定した位置（列）に対応する共有情報（ｎ）の一部（ｋ）を捨てることを特徴とする請求項２に記載の量子鍵配送方法。

【請求項６】　前記暗号鍵生成ステップにあっては、前記共有情報（ｎ）の一部（ｋ）を捨てた後、一方の装置が、正則なランダム行列Ｒ（（ｎ－ｋ）×（ｎ－ｋ））を生成し、公開通信路を介して他方の通信装置に通知し、前記第１お

よび第２の通信装置が、それぞれ前記ランダム行列Ｒを暗号鍵に作用させることを特徴とする請求項３、４または５に記載の量子鍵配送方法。

【請求項７】　光子を量子通信路上に送信する通信装置において、

受信側の通信装置と同一のパリティ検査行列Ｈ（ｎ×ｋ）を生成する検査行列生成手段と、

乱数列（送信データ）を発生し、所定の送信コード（基底）をランダムに決定し、当該送信データと送信コードの組み合わせによって規定された量子状態で光子を量子通信路上に送信し、その後、前記受信側の通信装置における測定が正しい測定器で行われたものかどうかを調べ、正しい測定器で測定されたｎビットの送信データを残し、その他を捨てる送信手段と、

前記パリティ検査行列Ｈとｎビットの送信データに基づくｋビットの誤り訂正情報を、公開通信路を介して前記受信側の通信装置に通知する誤り訂正情報通知手段と、

公開した誤り訂正情報に応じて誤り訂正後の共有情報（ｎ）の一部（ｋ）を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を受信側の通信装置との共有鍵とする暗号鍵生成手段と、

を備えることを特徴とする通信装置。

【請求項８】　量子通信路上の光子を測定する通信装置において、

送信側の通信装置と同一のパリティ検査行列Ｈ（ｎ×ｋ）を生成する検査行列生成手段と、

所定の受信コード（基底）をランダムに決定し、量子通信路上の光子を測定し、前記受信コードと測定結果の組み合わせによって規定された受信データを再生し、その後、前記測定が正しい測定器で行われたものかどうかを調べ、正しい測定器で測定されたｎビットの受信データを残し、その他を捨てる受信手段と、

公開通信路を介して受信したｋビットの誤り訂正情報と、前記パリティ検査行列Ｈとｎビットの受信データと、に基づいて、受信データの誤りを訂正する誤り訂正手段と、

公開された誤り訂正情報に応じて誤り訂正後の共有情報（ｎ）の一部（ｋ）を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を送信側の通信装置との共有

鍵とする暗号鍵生成手段と、

を備えることを特徴とする通信装置。

【請求項９】　前記検査行列生成手段は、

基本行列として有限アフィン幾何を用い、ガウス近似法による最適化を行うことによって、パリティ検査行列の最適な行と列の重み配分を探索し、

前記最適な重み配分に基づいて、前記有限アフィン幾何の行および列の重みを所定の手順でランダムに分割し、

列と行の重みまたはどちらか一方が均一でない低密度パリティ検査符号のパリティ検査行列Ｈを生成することを特徴とする請求項７または８に記載の通信装置。

【請求項１０】　前記検査行列生成手段は、さらに、「ＨＧ＝０」を満たす生成行列Ｇ（（ｎ－ｋ）×ｎ）から、$G^{-1}\cdot G=I$（単位行列）となる逆行列G^{-1}（ｎ×（ｎ－ｋ））を生成し、

前記暗号鍵生成手段は、逆行列G^{-1}を用いて共有情報（ｎ）の一部（ｋ）を捨てることを特徴とする請求項７、８または９に記載の通信装置。

【請求項１１】　前記検査行列生成手段は、さらに、ｎ次元ベクトルをｍ（ｍ≦ｎ－ｋ）次元ベクトルに写す写像Ｆで、任意のｍ次元ベクトルｖに対して、写像Ｆと「ＨＧ＝０」を満たす生成行列Ｇの合成写像Ｆ・Ｇにおける逆像$(F\cdot G)^{-1}(v)$の元の個数がｖによらず一定（2^{n-k-m}）であるものを生成し、

前記暗号鍵生成手段は、写像Ｆを用いて共有情報（ｎ）の一部を捨てることを特徴とする請求項７、８または９に記載の通信装置。

【請求項１２】　前記暗号鍵生成手段にあっては、前記パリティ検査行列Ｈの列に対してランダム置換を実行し、前記パリティ検査行列Ｈの生成元の有限アフィン幾何ＡＧ（２，2^s）の１列目の中から特定の「１」を選び、その位置を、公開通信路を介して交換し、前記置換後のパリティ検査行列から前記「１」に対応する分割後の位置（列）、および巡回シフトされた各列における前記「１」に対応する分割後の位置（列）、を特定し、その特定した位置（列）に対応する共有情報（ｎ）の一部（ｋ）を捨てることを特徴とする請求項９に記載の通信装置。

【請求項１３】　前記暗号鍵生成手段は、前記共有情報（ｎ）の一部（ｋ）を捨てた後、正則なランダム行列Ｒ（（ｎ－ｋ）×（ｎ－ｋ））を前記暗号鍵に作用させることを特徴とする請求項１０、１１または１２に記載の通信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法に関するものであり、特に、誤り訂正符号を用いてデータ誤りを訂正可能な量子鍵配送方法および当該量子鍵配送を実現可能な通信装置に関するものである。

【０００２】

【従来の技術】

以下、従来の量子暗号システムについて説明する。近年、高速大容量な通信技術として光通信が広く利用されていが、このような光通信システムでは、光のオン／オフで通信が行われ、オンのときに大量の光子が送信されているため、量子効果が直接現れる通信系にはなっていない。

【０００３】

一方、量子暗号システムでは、通信媒体として光子を用い、不確定性原理等の量子効果が生じるように１個の光子で１ビットの情報を伝送する。このとき、盗聴者が、その偏光，位相等の量子状態を知らずに適当に基底を選んで光子を測定すると、その量子状態に変化が生じる。したがって、受信側では、この光子の量子状態の変化を確認することによって、伝送データが盗聴されたかどうかを認識することができる。

【０００４】

図９は、従来の偏光を利用した量子鍵配送の概要を示す図である。たとえば、水平垂直方向の偏光を識別可能な測定器では、量子通信路上の、水平方向（０°）に偏光された光と垂直方向（９０°）に偏光された光とを正しく識別する。一方、斜め方向（４５°，１３５°）の偏光を識別可能な測定器では、量子通信路上の、４５°方向に偏光された光と１３５°方向に偏光された光とを正しくを識

別する。

【０００５】

このように、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（０°，９０°）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ５０％の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

【０００６】

図９に示す従来の量子鍵配送では、上記不確定性（ランダム性）を利用して、盗聴者に知られずに送信者と受信者との間で鍵を共有する（たとえば、非特許文献１参照。）。なお、送信者および受信者は、量子通信路以外に公開通信路を使用することができる。ここで、鍵の共有手順について説明する。

【０００７】

まず、送信者は、乱数列（１，０の列：送信データ）を発生し、さらに送信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応，×：斜め方向に偏光された光を識別可能な測定器に対応）をランダムに決定する。その乱数列と送信コードの組み合わせで、送信する光の偏光方向が自動的にきまる。ここでは、０と＋の組み合わせで水平方向に偏光された光を、１と＋の組み合わせで垂直方向に偏光された光を、０と×の組み合わせで４５°方向に偏光された光を、１と×の組み合わせで１３５°方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。

【０００８】

つぎに、受信者は、受信コード（＋：水平垂直方向に偏光された光を識別可能な測定器，×：斜め方向に偏光された光を識別可能な測定器）をランダムに決定し、量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組み合わせによって受信データを得る。ここでは、受信データとして、水平方向に偏光された光と＋の組み合わせで０を、垂直方向に偏光された光と＋の組み合わせで１を、４５°方向に偏光された光と×の組み合わせで０を、１３５°方

向に偏光された光と×の組み合わせで０を、それぞれ得る。

【０００９】

つぎに、受信者は、自身の測定が正しい測定器で行われたものかどうかを調べるために、受信コードを、公開通信路を介して送信者に対して送信する。受信コードを受け取った送信者は、正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信者に対して返信する。

【００１０】

つぎに、受信者は、正しい測定器で受信した受信信号に対応する受信データだけを残し、その他を捨てる。この時点で、残された受信データは送信者と受信者との間で確実に共有できている。

【００１１】

つぎに、送信者と受信者は、それぞれの通信相手に対して、共有データから選択した所定数のデータを、公開通信路を経由して送信する。そして、受け取ったデータが自信の持つデータと一致しているかどうかを確認する。たとえば、確認したデータの中に一致しないデータが１つでもあれば、盗聴者がいるものと判断して共有データを捨て、再度、鍵の共有手順を最初からやり直す。一方、確認したデータがすべて一致した場合には、盗聴者がいないと判断し、確認に使用したデータを捨て、残った共有データを送信者と受信者の共有鍵とする。

【００１２】

また、上記従来の量子鍵配送方法の応用として、たとえば、伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法がある（たとえば、非特許文献２参照。）。

【００１３】

この方法では、送信者が、データ誤りを検出するために、送信データを複数のブロックに分割し、ブロック毎のパリティを公開通信路上に送信する。そして、受信者が、公開通信路を経由して受け取ったブロック毎のパリティと受信データにおける対応するブロックのパリティとを比較して、データ誤りをチェックする。このとき、異なるパリティがあった場合、受信者は、どのブロックのパリティが異なっているのかを示す情報を公開通信路上に返信する。そして、送信者は、

該当するブロックをさらに前半部のブロックと後半部のブロックに分割し、たとえば、前半部のパリティを公開通信路上に返信する（二分探索）。以降、送信者と受信者は、上記二分探索を繰り返し実行することによりエラービットの位置を特定し、最終的に受信者がそのビットを訂正する。

【００１４】

さらに、送信者は、データに誤りがあるにもかかわらず、偶数個の誤りのために正しいと判定されたパリティがある場合を想定し、送信データをランダムに並べ替えて（ランダム置換）複数のブロックに分割し、再度、上記二分探索による誤り訂正処理を行う。そして、ランダム置換によるこの誤り訂正処理を繰り返し実行することによって、すべてのデータ誤りを訂正する。

【００１５】

【非特許文献１】

Bennett, C. H. and Brassard, G.: Quantum Cryptography: Public Key Distribution and Coin Tossing, In Proceedings of IEEE Conference on Computers, System and Signal Processing, Bangalore, India, pp.175-179 (DEC.1984).

【非特許文献２】

Brassard, G. and Salvail, L. 1993 Secret-Key Reconciliation by Public Discussion, In Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Computer Science 765, 410-423.

【００１６】

【発明が解決しようとする課題】

しかしながら、上記図９に示す従来の量子鍵配送においては、誤り通信路を想定していないため、誤りがある場合には盗聴行為が存在したものとして上記共通データ（共通鍵）を捨てることとなり、伝送路によっては共通鍵の生成効率が非常に悪くなる、という問題があった。

【００１７】

また、上記伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法においては、エラービットを特定するために膨大な回数のパリティのやりとりが発生し、さらに、ランダム置換による誤り訂正処理が所定回数にわたって行われるため、

誤り訂正処理に多大な時間を費やすことになる、という問題があった。

【００１８】

本発明は、上記に鑑みてなされたものであって、極めて高い特性を持つ誤り訂正符号を用いて伝送路上におけるデータ誤りを訂正しつつ、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法を得ることを目的とする。

【００１９】

【課題を解決するための手段】

上述した課題を解決し、目的を達成するために、本発明にかかる量子鍵配送方法にあっては、光子を量子通信路上に送信する第１の通信装置と当該光子を測定する第２の通信装置で構成された量子暗号システムにて実行され、たとえば、前記第１および第２の通信装置が、同一のパリティ検査行列Ｈ（ｎ×ｋ）を生成する検査行列生成ステップと、前記第１の通信装置が、乱数列（送信データ）を発生し、さらに所定の送信コード（基底）をランダムに決定し、前記第２の通信装置が、所定の受信コード（基底）をランダムに決定する乱数発生ステップと、前記第１の通信装置が、前記送信データと送信コードの組み合わせによって規定された量子状態で、光子を量子通信路上に送信する光子送信ステップと、前記第２の通信装置が、量子通信路上の光子を測定し、前記受信コードと測定結果の組み合わせによって規定された受信データを得る光子受信ステップと、前記第１および第２の通信装置が、前記測定が正しい測定器で行われたものかどうかを調べ、正しい測定器で測定されたｎビットの受信データおよび対応する送信データを残し、その他を捨てるデータ削除ステップと、前記第１の通信装置が、前記パリティ検査行列Ｈとｎビットの送信データに基づくｋビットの誤り訂正情報を、公開通信路を介して前記第２の通信装置に通知する誤り訂正情報通知ステップと、前記第２の通信装置が、前記パリティ検査行列Ｈとｎビットの受信データと誤り訂正情報に基づいて、受信データの誤りを訂正する誤り訂正ステップと、前記第１および第２の通信装置が、公開された誤り訂正情報に応じて誤り訂正後の共有情報（ｎ）の一部（ｋ）を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を装置間の共有鍵とする暗号鍵生成ステップと、を含むことを特徴とする。

【００２０】

この発明によれば、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、さらに、公開された誤り訂正情報に応じて共有情報の一部を捨てる。

【００２１】

【発明の実施の形態】

以下に、本発明にかかる量子鍵配送方法の実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。また、以下では、例として偏光を利用する量子鍵配送について説明するが、本発明は、たとえば、位相を利用するもの，周波数を利用するもの等にも適用可能であり、どのような量子状態を利用するかについては特に限定しない。

【００２２】

実施の形態１．

量子鍵配送は、盗聴者の計算能力によらず、安全性の保証された鍵配送方式であるが、たとえば、より効率よく共有鍵を生成するためには、伝送路を通ることによって発生するデータの誤りを取り除く必要がある。そこで、本実施の形態では、極めて高い特性をもつことが知られている低密度パリティ検査（ＬＤＰＣ：：Low-Density Parity-Check）符号を用いて誤り訂正を行う量子鍵配送について説明する。

【００２３】

図１は、本発明にかかる量子暗号システムにおける通信装置（送信機，受信機）の構成を示す図である。この量子暗号システムは、情報m_Aを送信する機能を備えた送信側の通信装置と、伝送路上で雑音等の影響を受けた情報m_A、すなわち情報m_Bを受信する機能を備えた受信側の通信装置と、から構成される。

【００２４】

また、送信側の通信装置は、量子通信路を介して情報m_Aを送信し、公開通信路を介してシンドロームs_Aを送信し、これらの送信情報に基づいて暗号鍵（受信側との共通鍵）を生成する暗号鍵生成部１と、暗号化部２１が暗号鍵に基づいて暗号化したデータを、送受信部２２が公開通信路を介してやりとりする通信部２と、を備え、受信側の通信装置は、量子通信路を介して情報m_Bを受信し、公

開通信路を介してシンドロームs_Aを受信し、これらの受信情報に基づいて暗号鍵（送信側との共通鍵）を生成する暗号鍵生成部３と、暗号化部４２が暗号鍵に基づいて暗号化したデータを、送受信部４１が公開通信路を介してやりとりする通信部４と、を備える。

【００２５】

上記送信側の通信装置では、量子通信路上に送信する情報m_Aとして、偏光フィルターを用いて所定の方向に偏光させた光（図９参照）を、受信側の通信装置に対して送信する。一方、受信側の通信装置では、水平垂直方向（０°，９０°）の偏光を識別可能な測定器と斜め方向（４５°，１３５°）の偏光を識別可能な測定器とを用いて、量子通信路上の、水平方向（０°）に偏光された光と垂直方向（９０°）に偏光された光と４５°方向に偏光された光と１３５°方向に偏光された光とを識別する。なお、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（０°，９０°）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ５０％の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

【００２６】

以下、上記量子暗号システムにおける各通信装置の動作、すなわち、本実施の形態における量子鍵配送について詳細に説明する。図２は、本実施の形態の量子鍵配送を示すフローチャートであり、詳細には、（ａ）は送信側の通信装置の処理を示し、（ｂ）は受信側の通信装置の処理を示す。

【００２７】

まず、上記送信側の通信装置および受信側の通信装置では、パリティ検査行列生成部１０，３０が、特定の線形符号のパリティ検査行列Ｈ（ｎ×ｋ）を求め、このパリティ検査行列Ｈから「ＨＧ＝０」を満たす生成行列Ｇ（（ｎ－ｋ）×ｎ）を求め、さらに、$G^{-1}\cdot G=I$（単位行列）となるＧの逆行列G^{-1}（ｎ×（ｎ－ｋ））を求める（ステップＳ１，ステップＳ１１）。本実施の形態では、上記特定の線形符号として、シャノン限界に極めて近い優れた特性をもつＬＤＰＣ符

号を用いた場合の量子鍵配送について説明する。なお、本実施の形態では、誤り訂正方式としてＬＤＰＣ符号を用いることとしたが、これに限らず、たとえば、ターボ符号等の他の線形符号を用いることとしてもよい。また、たとえば、後述する誤り訂正情報（シンドローム）が適当な行列Ｈと情報m_Aの積Ｈm_Aで表される誤り訂正プロトコル（たとえば、従来技術にて説明した「伝送路上におけるデータ誤りを訂正可能な量子鍵配送」に相当する誤り訂正プロトコル）であれば、すなわち、誤り訂正情報と情報m_Aの線形性が確保されるのであれば、その行列Ｈを用いることとしてもよい。

【００２８】

ここで、上記パリティ検査行列生成部１０におけるＬＤＰＣ符号の構成法について、詳細には、有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法（図２ステップＳ１の詳細）について説明する。図３は、有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法を示すフローチャートである。なお、パリティ検査行列生成部３０については、パリティ検査行列生成部１０と同様に動作するのでその説明を省略する。また、本実施の形態における検査行列生成処理は、たとえば、設定されるパラメータに応じてパリティ検査行列生成部１０で実行する構成としてもよいし、通信装置外部の他の制御装置（計算機等）で実行することとしてもよい。本実施の形態における検査行列生成処理が通信装置外部で実行される場合は、生成済みの検査行列が通信装置に格納される。以降の実施の形態では、パリティ検査行列生成部１０で上記処理を実行する場合について説明する。

【００２９】

まず、パリティ検査行列生成部１０では、「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用の検査行列のベースとなる有限アフィン幾何符号ＡＧ（２，2^s）を選択する（図３、ステップＳ２１）。ここでは、行の重みと列の重みがそれぞれ2^sとなる。図４は、たとえば、有限アフィン幾何符号ＡＧ（２，$2^{2)}$）のマトリクスを示す図（空白は０を表す）である。

【００３０】

つぎに、パリティ検査行列生成部１０では、列の重みの最大値r_1（$2 < r_1 \leq$

2^s）を決定する（ステップＳ２２）。そして、符号化率ｒａｔｅ（１－シンドローム長／鍵の長さ）を決定する（ステップＳ２２）。

【００３１】

つぎに、パリティ検査行列生成部１０では、ガウス近似法（Gaussian Approximation）による最適化を用いて、暫定的に、列の重み配分λ（γ_i）と行の重み配分ρ_μを求める（ステップＳ２３）。なお、行の重み配分の生成関数ρ（ｘ）は$\rho(x)=\rho_\mu x^{\mu-1}+(1-\rho_\mu)x^\mu$とする。また、重みμはμ≧２の整数であり、$\rho_\mu$は行における重みμの割合を表す。

【００３２】

つぎに、パリティ検査行列生成部１０では、有限アフィン幾何の行の分割により構成可能な、行の重み｛μ，μ＋１｝を選択し、さらに（１）式を満たす分割係数｛b_μ，$b_{\mu+1}$｝を求める（ステップＳ２４）。なお、b_μ，$b_{\mu+1}$は非負の整数とする。

$$b_\mu+b_{\mu+1}(\mu+1)=2^s \quad \cdots(1)$$

【００３３】

具体的には、下記（２）式からb_μを求め、上記（１）式から$b_{\mu+1}$を求める。

【００３４】

【数１】

$$\arg\cdot\min_{b\mu}\left|\varphi_\mu-\frac{\mu\times b_\mu}{2^s}\right| \quad \cdots \quad (2)$$

【００３５】

つぎに、パリティ検査行列生成部１０では、上記決定したパラメータμ，μ＋１，b_μ，$b_{\mu+1}$によって（上記行の分割処理によって）更新された行の重みの比率ρ_μ'，$\rho_{\mu+1}'$を（３）式により求める（ステップＳ２５）。

【００３６】

【数２】

$$\varphi'_{\mu}=\frac{\mu\times b_{\mu}}{2^{s}}$$
$$\varphi'_{\mu+1}=\frac{(\mu+1)\times b_{\mu+1}}{2^{s}} \qquad \cdots \quad (3)$$

【００３７】

つぎに、パリティ検査行列生成部１０では、ガウス近似法による最適化を用いて、さらに上記で求めたμ，$\mu+1$，$\rho\mu'$，$\rho\mu_{+1}'$を固定のパラメータとして、暫定的に、列の重み配分λ（γ_i）を求める（ステップＳ２６）。なお、重みγ_iは$\gamma_i\geqq 2$の整数であり、λ（γ_i）は列における重みγ_iの割合を表す。また、列数が１以下となる重み（λ（γ_i）$\leqq\gamma_i/w_t$，ｉは正の整数）を候補から削除する。ただし、w_tはＡＧ（２，2^s）に含まれる１の総数を表す。

【００３８】

つぎに、上記で求めた重み配分を満たし、かつ下記（４）式を満たす、列の重み候補のセット｛γ_1，γ_2，…γ_l（$\gamma_l\leqq 2^s$）｝を選択する（ステップＳ２７）。そして、下記の（４）式を満たさない列の重みγ_iが存在する場合には、その列の重みを候補から削除する。

【００３９】

【数３】

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,\ell} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,\ell} \\ \vdots & & \cdots & \vdots \end{bmatrix}\begin{bmatrix}\gamma_1\\ \gamma_2\\ \vdots\\ \gamma_\ell\end{bmatrix}=\begin{bmatrix}2^s\\ 2^s\\ \vdots\\ 2^s\end{bmatrix} \qquad \cdots \quad (4)$$

【００４０】

なお、各ａは、列の重み2^sを構成するための｛γ_1，γ_2，…γ_l｝に対する非負の整数となる係数を表し、ｉ，ｊは正の整数であり、γ_iは列の重みを表し、γ_iは列の最大重みを表す。

【００４１】

つぎに、パリティ検査行列生成部１０では、ガウス近似法による最適化を用いて、さらに上記で求めたμ，$\mu+1$，$\rho\mu'$，$\rho\mu+1'$と$\{\gamma 1, \gamma 2, \cdots \gamma 1\}$を固定パラメータとして、列の重み配分$\lambda$（$\gamma_i$）と行の重み配分$\rho\mu$を求める（ステップＳ２８）。

【００４２】

つぎに、パリティ検査行列生成部１０では、分割処理を行う前に、列の重み配分λ（γ_i）と行の重み配分$\rho\mu$を調整する（ステップＳ２９）。なお、調整後の各重みの配分は、可能な限りガウス近似法で求めた値に近い値にする。図５は、ステップＳ２９における最終的な列の重み配分λ（γ_i）と行の重み配分$\rho\mu$を示す図である。

【００４３】

最後に、パリティ検査行列生成部１０では、有限アフィン幾何における行および列を分割して（ステップＳ３０）、ｎ×ｋのパリティ検査行列Ｈを生成する。本発明における有限アフィン幾何符号の分割処理は、規則的に分割するのではなく、各行または各列から「１」の番号をランダムに抽出する（後述するランダム分割の具体例を参照）。なお、この抽出処理は、ランダム性が保持されるのであればどのような方法を用いてもよい。

【００４４】

具体的にいうと、ＥＧ（２，2^5）における１列中の「１」の行番号が、

$B_1(x) = \{1\ 32\ 114\ 136\ 149\ 223\ 260\ 382\ 402\ 438\ 467\ 507\ 574\ 579\ 588\ 622\ 634\ 637\ 638\ 676\ 717\ 728\ 790\ 851\ 861\ 879\ 947\ 954\ 971\ 977\ 979\ 998\}$

の場合、分割後の行列における１～４列目$R_m(n)$は、$B_1(x)$から「１」の番号がランダムに抽出され、たとえば、

$R_1(n) = \{1\ 114\ 574\ 637\ 851\ 879\ 977\ 979\}$

$R_2(n) = \{32\ 136\ 402\ 467\ 588\ 728\ 861\ 971\}$

$R_3(n) = \{149\ 260\ 382\ 438\ 579\ 638\ 717\ 998\}$

$R_4(n) = \{223\ 507\ 622\ 634\ 676\ 790\ 947\ 954\}$

となる。

【００４５】

ここで、上記ランダム分割の一例、すなわち、上記「乱数系列のラテン方陣を用いた分割方法」を詳細に説明する。ここでは、ランダム分割を行う場合のランダム系列を容易かつ確定的に生成する。この方法による利点は、送信側と受信側が同じランダム系列を生成できることにある。

【００４６】

（１）基本のランダム系列を作成する。ここでは、有限アフィン幾何ＡＧ（２，2^s）を用い、ＰをＰ≧2^sを満たす最小の素数とした場合の、基本のランダム系列Ｃ（ｉ）を（５）式にしたがって作成する。

Ｃ（１）＝１

Ｃ（ｉ＋１）＝G_0×Ｃ（ｉ）　ｍｏｄ　Ｐ　　…（５）

なお、ｉ＝０，１，…，Ｐ－２とし、G_0はガロア体ＧＦ（Ｐ）の原始元である。また、系列長が2^sとなるように、2^sより大きい数をＣ（ｉ）の中から削除し、削除後のＣ（ｉ）を基本のランダム系列とする。

【００４７】

（２）基本のランダム系列Ｃ（ｉ）を一定間隔で読み出すためにスキップ間隔Ｓ（ｊ）を以下の（６）式のように定義する。

Ｓ（ｊ）＝ｊ　　ｊ＝１，２，…，2^s　　…（６）

【００４８】

（３）以下の（７）式で置換パターンLB_j（ｉ）を作成する。

LB_j（ｉ）＝（（Ｓ（ｊ）×ｉ）　ｍｏｄ　Ｐ）＋１

ｊ＝１，２，…，2^s

ｉ＝１，２，…，Ｐ－１　　…（７）

なお、LB_j（ｉ）も2^sより大きい数字は削除する。

【００４９】

（４）ｑ列ｉ行でｊ番目のラテン方陣行列L_{jq}（ｉ）を以下の（８）式で算出する。

L_{jq}（ｉ）＝LB_j（（（ｑ＋ｉ－２）　ｍｏｄ　2^s）＋１）

ｊ＝１，２，…，2^s

$i = 1, 2, \cdots, 2^s$

$q = 1, 2, \cdots, 2^s$　　…（８）

【００５０】

（５）ラテン方陣行列L_{jq}（ｉ）にしたがって列と行を分割する。列の分割では、$g_0, g_0, \cdots, g_{n-1}$をパリティ検査行列Ｈの列ベクトルとし、$g_c'$（ｋ）を$g_c$，ｃ＝０，１，…，ｎ－１の列の中のｋ番目の「１」とする。また、g_cの中の「１」の位置の集合をG_cとする（（９）式参照）。

$G_c = \{g_c'(k), k = 1, 2, \cdots, 2^s\}$　　…（９）

たとえば、ＡＧ（２，2^3）のｃ＝１番目の列の「１」の行番号は、$G_1 = \{1\ 3\ 8\ 20\ 23\ 24\ 34\ 58\}$ となる。そして、このｃ列目の列ベクトルをg_c'（ｋ）で表現すると、（１０）式のように表すことができる。

$g_c'(1) = ((c-1)+1) \bmod (2^{2s}-1)$

$g_c'(2) = (g_c'(1)+2) \bmod (2^{2s}-1)$

$g_c'(3) = (g_c'(2)+5) \bmod (2^{2s}-1)$

$g_c'(4) = (g_c'(3)+12) \bmod (2^{2s}-1)$

$g_c'(5) = (g_c'(4)+3) \bmod (2^{2s}-1)$

$g_c'(6) = (g_c'(5)+1) \bmod (2^{2s}-1)$

$g_c'(7) = (g_c'(6)+10) \bmod (2^{2s}-1)$

$g_c'(8) = (g_c'(7)+24) \bmod (2^{2s}-1)$　　…（１０）

【００５１】

ここで、パリティ検査行列Ｈの各列g_cを、上記（４）式を満たす列の次数と係数に基づいて、新しい列$g_{c,e}$に分割する。そして、$g_{c,e}'$（ｒ）を新しい列$g_{c,e}$の中のｒ行目の「１」とする。また、$g_{c,e}$の中の「１」の位置の集合を$G_{c,e}$とする（（１１）式参照）。

$G_{c,e} = \{g_{c,e}'(r), r = 1, 2, \cdots\}$　　…（１１）

【００５２】

そして、ラテン方陣行列群を用いて、下記（１２）式にしたがって分割するエッジの選択を行う。なお、$a_{t,1}, a_{t,2}, \cdots, a_{t,l}$と$\gamma_1, \gamma_2, \cdots, \gamma_l$は、上記式（４）を満たす係数と次数である。また、ｔは（４）式の係数行列の行番号を

示している。また、ｔ行目の式で分割する有限アフィン平面の列数をn_tとし、係数行列の行番号の最大値をt_mとすると、ｔは（１３）式で表すことができる。

【００５３】

【数４】

$$g'_{c,e}(r) = g'_c(L_{j,q}(i))$$
$$j = c/2^s$$
$$q = ((c-1) \bmod 2^s) + 1 \qquad \cdots (12)$$
$$i = r + \sum_{m=1}^{\ell} \min(a_{t,m}, \max(o, e-1-\sum_{n-1}^{m-1} a_{t,n})) \cdot \gamma_m$$

【００５４】

【数５】

$$t\begin{cases} 1 (1 \leqq c \leqq n_1) \\ 2 (n_1+1 \leqq c \leqq n_1+n_2) \\ \vdots \\ t_m (\sum_{i=1}^{tm-1} n_i + 1 \leqq c \leqq \sum_{i=2}^{tm} n_i) \end{cases} \cdots (13)$$

【００５５】

つぎに、上記（１）～（４）の分割処理を、具体例を挙げて説明する。例として、ＡＧ（２，2^3）のｃ＝１６番目の列の「１」の行番号をG_{16}＝｛10 16 18 23 35 38 39 49｝と定義する。図６は、ランダム系列のラテン方陣行列による分割手順を示す図である。図示のラテン方陣行列L_{jq}（ｉ）の結果を用いて手順（５）を実行すると、新しい列$g_{16,e}$の中の「１」は（１４）式のように表すことができる。

$g_{16,1}'$（１）＝g_{16}'（$L_{2,8}$（１））＝g_{16}'（３）＝１８

$g_{16,1}'$（２）＝g_{16}'（$L_{2,8}$（２））＝g_{16}'（２）＝１６

$g_{16,2}'(1)=g_{16}'(L_{2,8}(3))=g_{16}'(8)=49$

$g_{16,2}'(2)=g_{16}'(L_{2,8}(4))=g_{16}'(7)=39$

$g_{16,3}'(1)=g_{16}'(L_{2,8}(5))=g_{16}'(6)=38$

$g_{16,3}'(2)=g_{16}'(L_{2,8}(6))=g_{16}'(1)=10$

$g_{16,4}'(1)=g_{16}'(L_{2,8}(7))=g_{16}'(4)=23$

$g_{16,4}'(2)=g_{16}'(L_{2,8}(8))=g_{16}'(5)=35$　…（１４）

【００５６】

その結果、１６番目の列は以下のように分割される。

$G_{16,1}=\{18\ 16\}$

$G_{16,2}=\{49\ 39\}$

$G_{16,3}=\{38\ 10\}$

$G_{16,4}=\{23\ 35\}$

【００５７】

このように、本実施の形態では、上記有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法（図２、ステップＳ１）を実行することによって、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用の検査行列Ｈ（ｎ×ｋ）を生成することができる。

【００５８】

上記のように、パリティ検査行列Ｈ，生成行列Ｇ，G^{-1}（$G^{-1}\cdot G=I$：単位行列）を生成後、つぎに、送信側の通信装置では、乱数発生部１１が、乱数列（１，０の列：送信データ）を発生し、さらに送信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応したコード，×：斜め方向に偏光された光を識別可能な測定器に対応したコード）をランダムに決定する（ステップＳ２）。一方、受信側の装置では、乱数発生部３１が、受信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応したコード，×：斜め方向に偏光された光を識別可能な測定器に対応したコード）をランダムに決定する（ステップＳ１２）。

【００５９】

つぎに、送信側の通信装置では、光子生成部１２が、上記乱数列と送信コード

の組み合わせで自動的に決まる偏光方向で光子を送信する（ステップＳ３）。たとえば、０と＋の組み合わせで水平方向に偏光された光を、１と＋の組み合わせで垂直方向に偏光された光を、０と×の組み合わせで４５°方向に偏光された光を、１と×の組み合わせで１３５°方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。

【００６０】

光子生成部１２の光信号を受け取った受信側の通信装置の光子受信部３２では、量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組み合わせによって自動的に決まる受信データを得る（ステップＳ１３）。ここでは、受信データとして、水平方向に偏光された光と＋の組み合わせで０を、垂直方向に偏光された光と＋の組み合わせで１を、４５°方向に偏光された光と×の組み合わせで０を、１３５°方向に偏光された光と×の組み合わせで０を、それぞれ得る。

【００６１】

つぎに、受信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べるために、乱数発生部３１が、受信コードを、公開通信路を介して送信側の通信装置に対して送信する（ステップＳ１３）。受信コードを受け取った送信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信側の通信装置に対して送信する（ステップＳ３）。そして、受信側の通信装置および送信側の通信装置では、正しい測定器で受信した受信信号に対応するデータだけを残し、その他を捨てる（ステップＳ３，Ｓ１３）。その後、残ったデータをメモリ等に保存し、その先頭から順にｎビットを読み出し、送信データm_Aと受信データm_B（m_Bは伝送路上で雑音等の影響を受けたm_A）を生成する。すなわち、ここでは、共有鍵生成処理が終わる度につぎのｎビットを読み出し、その都度、送信データm_Aと受信データm_Bを生成する。本実施の形態では、正しい測定器で受信した受信信号に対応するビットの位置が、送信側の通信装置と受信側の通信装置との間で共有できている。

【００６２】

つぎに、送信側の通信装置では、シンドローム生成部１４が、パリティ検査行

列Ｈ（ｎ×ｋ）と送信データm_Aを用いてm_Aのシンドローム$S_A=Hm_A$を計算し、その結果を、公開通信路通信部１３，公開通信路を介して受信側の通信装置に通知する（ステップＳ４）。この段階で、m_AのシンドロームS_A（ｋビット分の情報）は盗聴者に知られる可能性がある。一方、受信側の通信装置では、公開通信路通信部３４にてm_AのシンドロームS_Aを受信し、それをシンドローム復号部３３に通知する（ステップＳ１４）。

【００６３】

シンドローム復号部３３では、パリティ検査行列Ｈと受信データm_Bを用いてm_Bのシンドローム$S_B=Hm_B$を計算し、さらに、m_AのシンドロームS_Aとm_BのシンドロームS_Bを用いてシンドローム$S=S_A+S_B$を計算する（ステップＳ１５）。そして、シンドロームＳに基づいて送信データm_Aを推定する（ステップＳ１６）。ここでは、$m_A=m_B+e$（雑音等）と仮定し、式（１５）に示すようにシンドロームＳを変形した後、シンドローム復号によりｅを求め、送信データm_Aを求める（ステップＳ１６）。なお、S_A+S_B，m_A+eの＋は排他的論理和を表す。

$$\begin{aligned} S&=S_A+S_B \\ &=Hm_A+Hm_B \\ &=H(m_A+m_B) \\ &=H(m_B+e+m_B) \\ &=He \qquad \cdots(15) \end{aligned}$$

【００６４】

最後に、受信側の通信装置では、共有鍵生成部３５が、公開された誤り訂正情報（盗聴された可能性のある上記ｋビット分の情報：S_A）に応じて共有情報（m_A）の一部を捨てて、ｎ－ｋビット分の情報量を備えた暗号鍵ｒを生成する（ステップＳ１７）。すなわち、共有鍵生成部３５では、先に計算しておいたG^{-1}（ｎ×（ｎ－ｋ））を用いて下記（１６）式により暗号鍵ｒを生成する。受信側の通信装置は、この暗号鍵ｒを送信側の通信装置との共有鍵とする。

$$r=G^{-1}m_A \qquad \cdots(16)$$

【００６５】

一方、送信側の通信装置においても、共有鍵生成部１５が、公開された誤り訂正情報（盗聴された可能性のある上記ｋビット分の情報：S_A）に応じて共有情報（m_A）の一部を捨てて、ｎ－ｋビット分の情報量を備えた暗号鍵ｒを生成する（ステップＳ５）。すなわち、共有鍵生成部１５では、先に計算しておいたG^{-1}（ｎ×（ｎ－ｋ））を用いて上記（１６）式により暗号鍵ｒを生成する（ステップＳ５）。送信側の通信装置は、この暗号鍵ｒを受信側の通信装置との共有鍵とする。

【００６６】

このように、本実施の形態おいては、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てる構成とした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる。また、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保証された共通鍵を生成することができる。

【００６７】

なお、本実施の形態では、ＨＧ＝０を満たす生成行列Ｇ（（ｎ－ｋ）×ｎ）から、$G^{-1}\cdot G=I$（単位行列）となる逆行列G^{-1}（ｎ×（ｎ－ｋ））を生成し、当該逆行列G^{-1}を用いて共有情報（ｎ）の一部（ｋ）を捨てて、ｎ－ｋビット分の情報量を備えた暗号鍵ｒを生成することとしたが、これに限らず、共有情報（ｎ）の一部を捨てて、ｍ（$m\leqq n-k$）ビット分の情報量を備えた暗号鍵ｒを生成することとしてもよい。具体的にいうと、ｎ次元ベクトルをｍ次元ベクトルに写す写像Ｆ（・）を想定する。Ｆ（・）は、共有鍵の安全性を保証するために、「任意のｍ次元ベクトルｖに対して、写像Ｆと生成行列Ｇの合成写像Ｆ・Ｇにおける逆像$(F\cdot G)^{-1}(v)$の元の個数がｖによらず一定（2^{n-k-m}）である」、という条件を満たす必要がある。このとき、共有鍵ｒは、ｒ＝Ｆ（m_A）となる。

【００６８】

実施の形態２．

実施の形態２では、前述した実施の形態１における暗号鍵の秘匿性をさらに増強させる。

【００６９】

図７は、本発明にかかる量子暗号システムの実施の形態２の構成を示す図である。なお、先に説明した実施の形態１と同様の構成については、同一の符号を付してその説明を省略する。量子通信路で盗聴された情報に対して秘匿性を増強させるためには、盗聴されたビット数分をハッシュ関数により圧縮する必要がある。しかしながら、ハッシュ関数は、その特性により盗聴されやすい位置が存在する。そこで、本実施の形態においては、その位置をランダムに並べ替えることによって対応する。

【００７０】

図８は、実施の形態２の量子鍵配送を示すフローチャートであり、詳細には、送信側の通信装置の処理を示す。送信側の通信装置のランダム置換部１６では、正則なランダム行列Ｒ（（ｎ－ｋ）×（ｎ－ｋ））を生成し、当該Ｒを共有鍵生成部１５に通知し、さらに、当該Ｒを、公開通信路を介して受信側の通信装置の共有鍵生成部３５に通知する（ステップＳ６）。なお、図７および図８では、一例として、送信側の通信装置でランダム行列Ｒを生成／送信しているが、これに限らず、この処理は、受信側の通信装置で行うこととしてもよい。

【００７１】

その後、送信側の通信装置では、共有鍵生成部１５が、公開された誤り訂正情報（盗聴された可能性のある上記ｋビット分の情報：S_A）に応じて共有情報（m_A）の一部を捨てて、さらに、受け取ったランダム行列Ｒを用いて秘匿性を増強して、ｎ－ｋビット分の情報量を備えた暗号鍵ｒを生成する（ステップＳ５）。すなわち、共有鍵生成部１５では、先に計算しておいたG^{-1}（ｎ×（ｎ－ｋ））と受け取ったランダム行列Ｒ（（ｎ－ｋ）×（ｎ－ｋ））を用いて下記（１７）式により暗号鍵ｒを生成する。送信側の通信装置は、この暗号鍵ｒを受信側の通信装置との共有鍵とする。

$$r = R G^{-1} m_A \qquad \cdots (17)$$

【００７２】

一方、受信側の通信装置においても、共有鍵生成部３５が、公開された誤り訂正情報（盗聴された可能性のある上記ｋビット分の情報：S_A）に応じて共有情報（m_A）の一部を捨てて、さらに、受け取ったランダム行列Ｒを用いて秘匿性を増強して、ｎ－ｋビット分の情報量を備えた暗号鍵ｒを生成する（ステップＳ１７）。すなわち、共有鍵生成部１５では、先に計算しておいたG^{-1}（ｎ×（ｎ－ｋ））と受け取ったランダム行列Ｒ（（ｎ－ｋ）×（ｎ－ｋ））を用いて上記（１７）式により暗号鍵ｒを生成する（ステップＳ１７）。受信側の通信装置は、この暗号鍵ｒを送信側の通信装置との共有鍵とする。

【００７３】

このように、本実施の形態おいては、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てて、さらに正則なランダム行列を用いて共有情報を並べ替える構成とした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる。また、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保証された共通鍵を生成することができる。さらに、正則なランダム行列を用いて共有情報を並べ替えることとしたため、秘匿性を増強させることができる。

【００７４】

なお、本実施の形態においても、実施の形態１と同様に、共有情報（ｎ）の一部を捨てて、ｍ（ｍ≦ｎ－ｋ）ビット分の情報量を備えた暗号鍵ｒを生成することとしてもよい。この場合、共有鍵ｒは、ｒ＝ＲＦ（m_A）となる。

【００７５】

実施の形態３．

先に説明した実施の形態１では、生成行列G^{-1}を用いて共有情報の一部を捨てていた。これに対して、実施の形態３では、生成行列G^{-1}を用いずに、パリティ検査行列Ｈの特性を用いて共有情報の一部を捨てる。なお、本実施の形態の構成

は、先に説明した実施の形態１の図１と同様である。

【００７６】

以下、実施の形態３の量子鍵配送について説明する。ここでは、先に説明した図２と異なる処理についてのみ説明する。

【００７７】

まず、上記送信側の通信装置および受信側の通信装置では、パリティ検査行列生成部１０，３０が、特定の線形符号のパリティ検査行列Ｈ（ｎ×ｋ）を求める（ステップＳ１，ステップＳ１１）。なお、有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法（図２ステップＳ１の詳細）については、先に説明した実施の形態１の図３と同様である。

【００７８】

そして、実施の形態１と同様の手順でステップＳ２～Ｓ４を実行後、受信側の通信装置では、共有鍵生成部３５が、公開された誤り訂正情報（盗聴された可能性のある上記ｋビット分の情報：S_A）に応じて共有情報（m_A）の一部を捨てて、ｎ－ｋビット分の情報量を備えた暗号鍵ｒを生成する（ステップＳ１７）。具体的には、共有鍵生成部３５が、上記ステップＳ１１で生成したパリティ検査行列の列に対してランダム置換を行う。そして、送信側の通信装置との間で捨てるビットに関する情報を、公開通信路を介して交換する。ここでは、元の有限アフィン幾何ＡＧ（２，2^S）の１列目の中から特定の「１」を選び、その位置を、公開通信路を介して交換する。

【００７９】

その後、共有鍵生成部３５では、上記置換後のパリティ検査行列から上記「１」に対応する分割後の位置、および巡回シフトされた各列における上記「１」に対応する分割後の位置を特定し、その特定した位置に対応する共有情報m_A内のビットを捨てて、残りのデータを暗号鍵ｒとする。受信側の通信装置は、この暗号鍵ｒを送信側の通信装置との共有鍵とする。

【００８０】

一方、送信側の通信装置においても、共有鍵生成部１５が、公開された誤り訂正情報（盗聴された可能性のある上記ｋビット分の情報：S_A）に応じて共有情

報（m_A）の一部を捨てて、ｎ－ｋビット分の情報量を備えた暗号鍵ｒを生成する（ステップＳ５）。具体的には、共有鍵生成部１５が、上記ステップＳ１で生成したパリティ検査行列の列に対して上記と同様のランダム置換を行う。そして、上記捨てるビットに関する情報を、公開通信路を介して交換する。

【００８１】

その後、共有鍵生成部１５では、上記置換後のパリティ検査行列から上記「１」に対応する分割後の位置、および巡回シフトされた各列における上記「１」に対応する分割後の位置を特定し、その特定した位置に対応する共有情報m_A内のビットを捨てて、残りのデータを暗号鍵ｒとする。送信側の通信装置は、この暗号鍵ｒを受信側の通信装置との共有鍵とする。

【００８２】

このように、本実施の形態においては、生成行列G^{-1}を用いずに、パリティ検査行列Ｈの特性を用いて共有情報の一部を捨てる構成とした。これにより、実施の形態１と同様の効果が得られるとともに、さらに、複雑な生成行列Ｇ，G^{-1}の演算処理を削除することができる。

【００８３】

なお、本実施の形態においては、パリティ検査行列Ｈの特性を用いて共有情報の一部を捨てて、さらに、実施の形態２と同様に、正則なランダム行列を用いて共有情報を並べ替える構成としてもよい。これにより、秘匿性を増強させることができる。

【００８４】

【発明の効果】

以上、説明したとおり、本発明によれば、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てることとした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる、という効果を奏する。また、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保

証された共通鍵を生成することができる、という効果を奏する。

【図面の簡単な説明】

【図１】　本発明にかかる量子暗号システムの実施の形態１の構成を示す図である。

【図２】　実施の形態２の量子鍵配送を示すフローチャートである。

【図３】　有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法を示すフローチャートである。

【図４】　有限アフィン幾何符号ＡＧ（２，2^2）のマトリクスを示す図である。

【図５】　最終的な列の重み配分λ（γ_i）と行の重み配分ρμを示す図である。

【図６】　ランダム系列のラテン方陣行列による分割手順を示す図である。

【図７】　本発明にかかる量子暗号システムの実施の形態２の構成を示す図である。

【図８】　実施の形態２の量子鍵配送を示すフローチャートである。

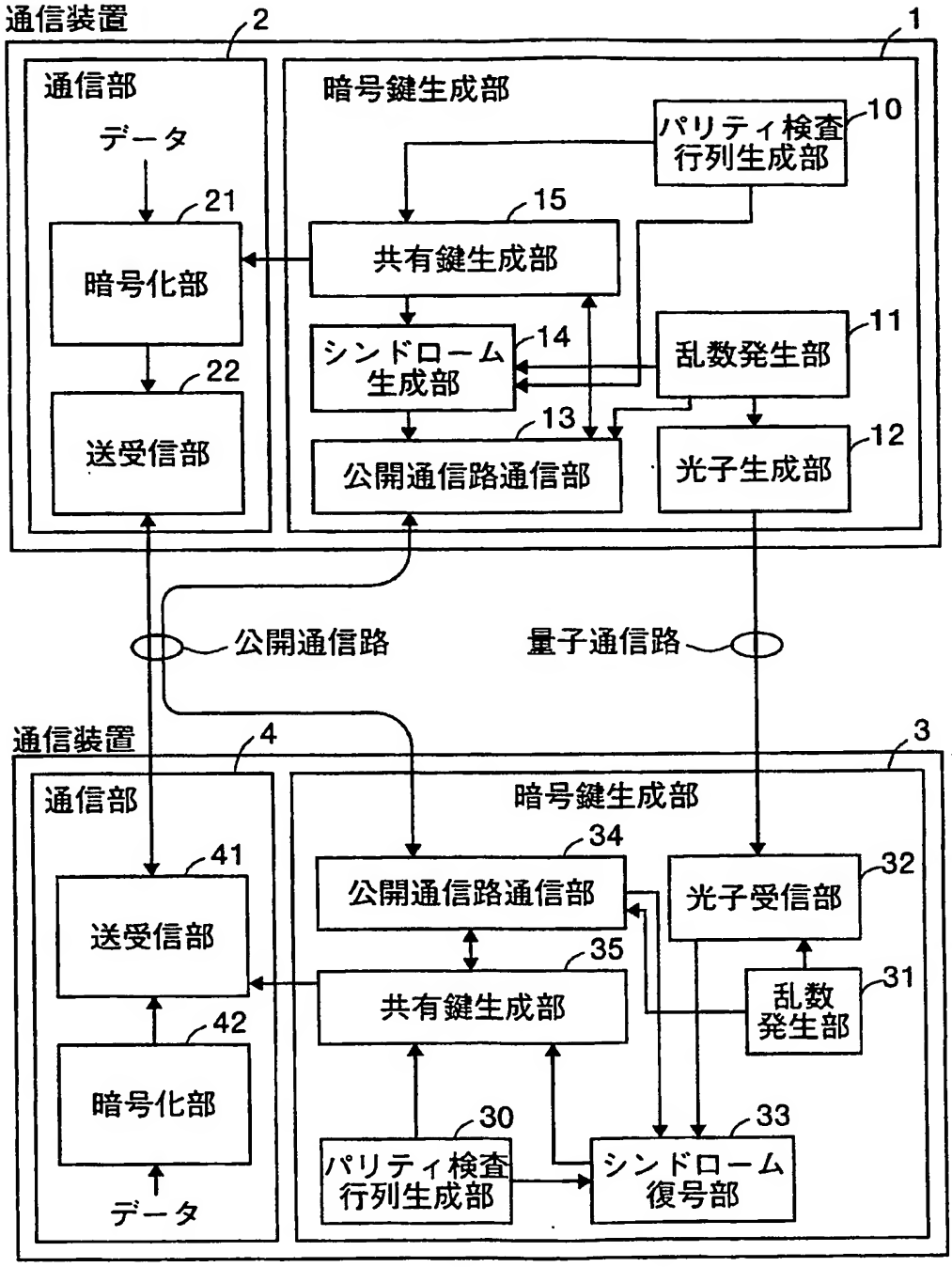
【図９】　従来の量子鍵配送の概要を示す図である。

【符号の説明】

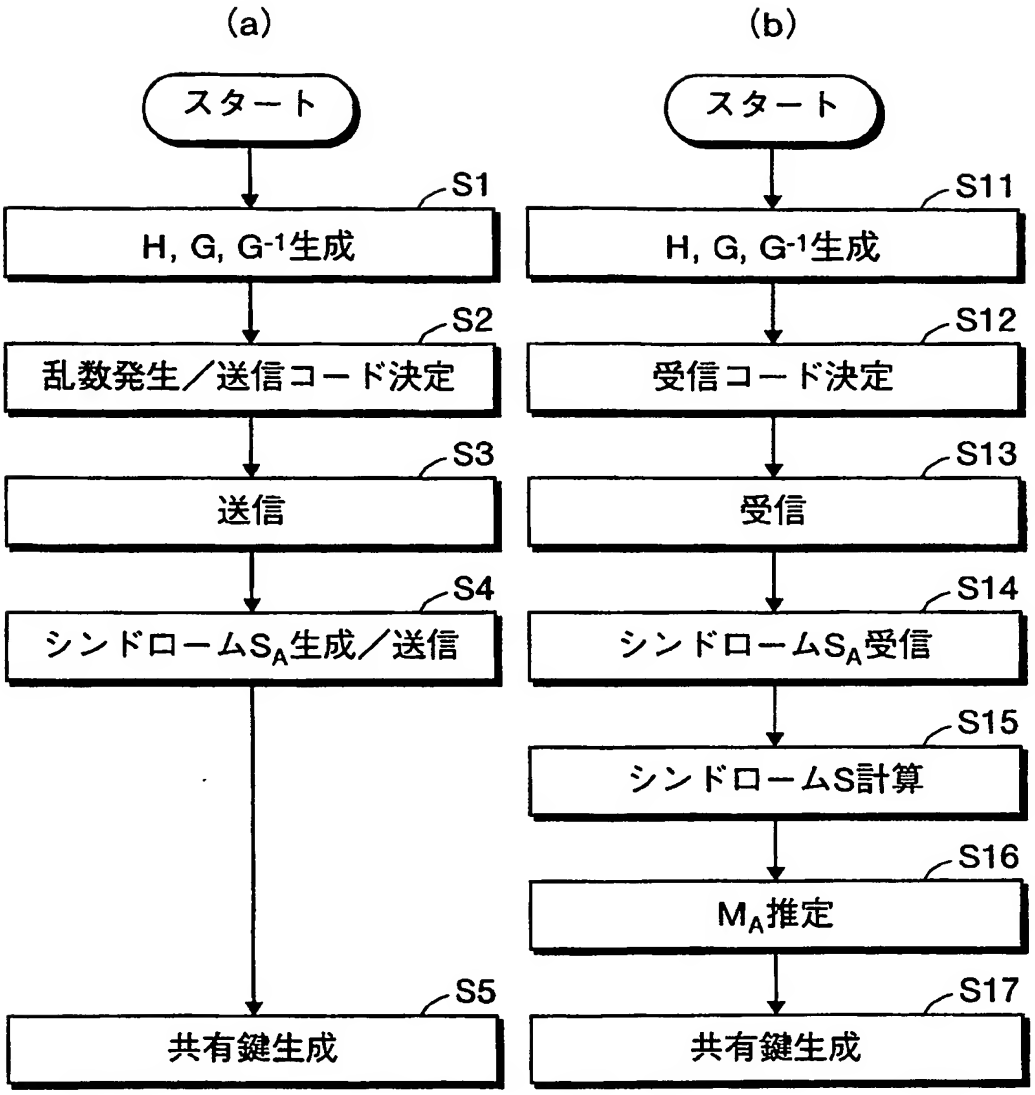
１，１ａ，３　暗号鍵生成部、２，４　通信部、１０，３０　パリティ検査行列生成部、１１，３１　乱数発生部、１２　光子生成部、１３，３４　公開通信路通信部、１４　シンドローム生成部、１５，３５　共有鍵生成部、２１，４２　暗号化部、２２，４１　送受信部、３２　光子受信部、３３　シンドローム復号部。

【書類名】　図面

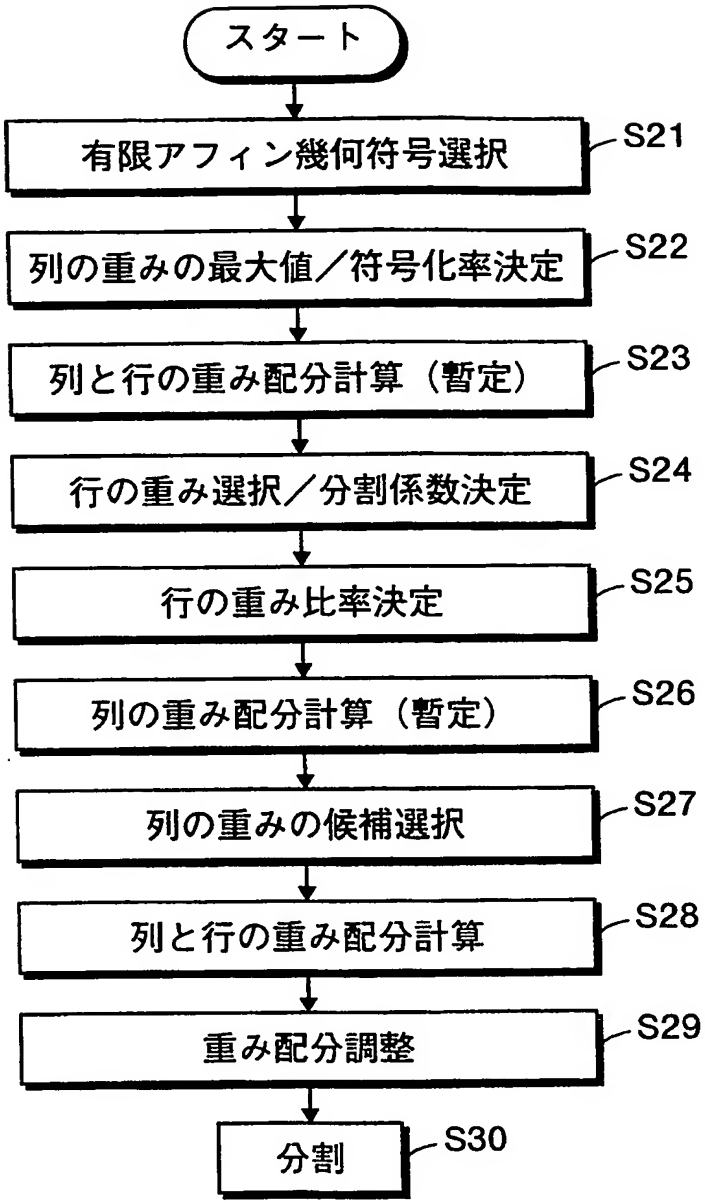
【図１】


通信装置
2
1
通信部
データ
21
暗号化部
22
送受信部
暗号鍵生成部
パリティ検査
行列生成部
10
15
共有鍵生成部
シンドローム
生成部
14
乱数発生部
11
13
公開通信路通信部
光子生成部
12
公開通信路
量子通信路
通信装置
4
3
通信部
41
送受信部
42
暗号化部
データ
暗号鍵生成部
34
公開通信路通信部
光子受信部
32
35
共有鍵生成部
乱数
発生部
31
30
パリティ検査
行列生成部
33
シンドローム
復号部

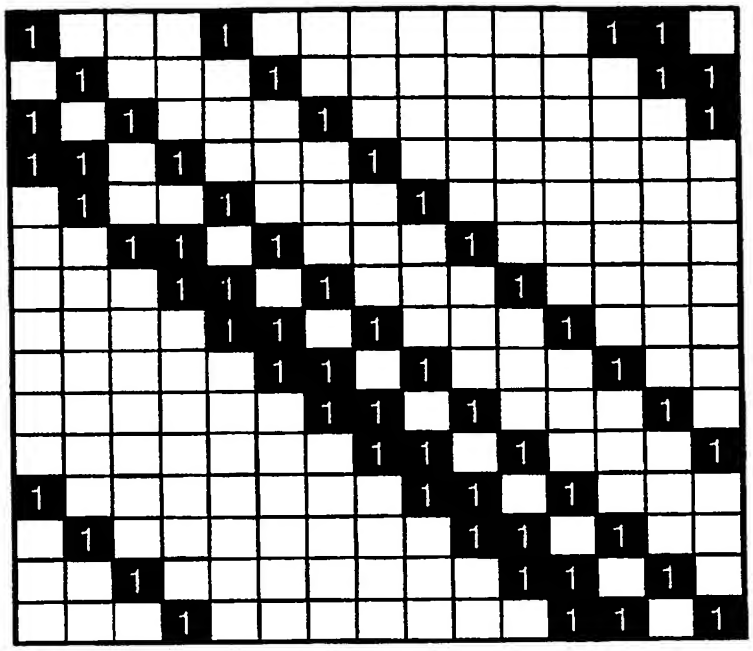
【図２】


(a)
スタート
S1
H, G, G-1生成
S2
乱数発生／送信コード決定
S3
送信
S4
シンドロームSA生成／送信
S5
共有鍵生成
(b)
スタート
S11
H, G, G-1生成
S12
受信コード決定
S13
受信
S14
シンドロームSA受信
S15
シンドロームS計算
S16
MA推定
S17
共有鍵生成

【図３】


スタート
有限アフィン幾何符号選択
S21
列の重みの最大値／符号化率決定
S22
列と行の重み配分計算（暫定）
S23
行の重み選択／分割係数決定
S24
行の重み比率決定
S25
列の重み配分計算（暫定）
S26
列の重みの候補選択
S27
列と行の重み配分計算
S28
重み配分調整
S29
分割
S30

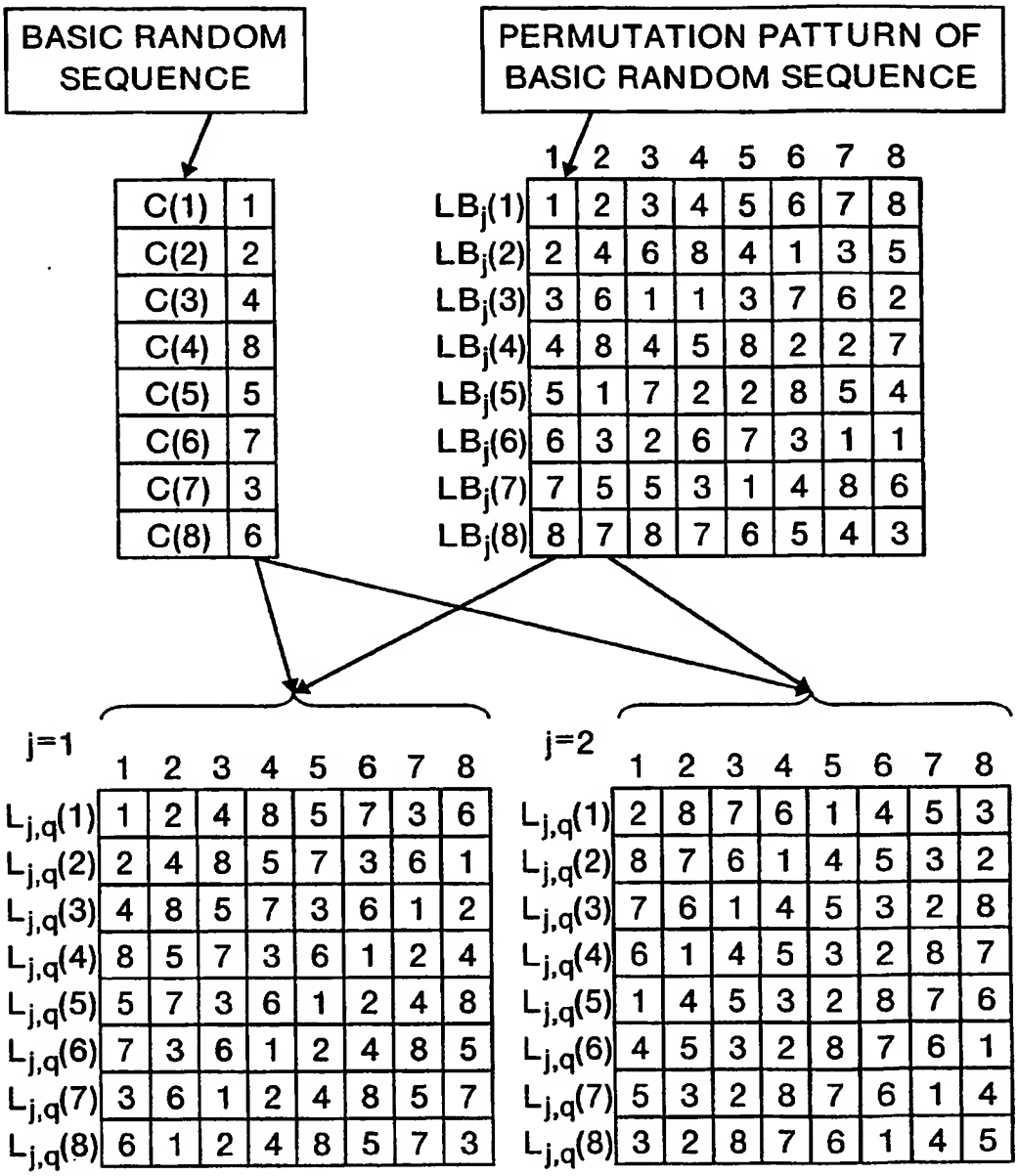
【図４】



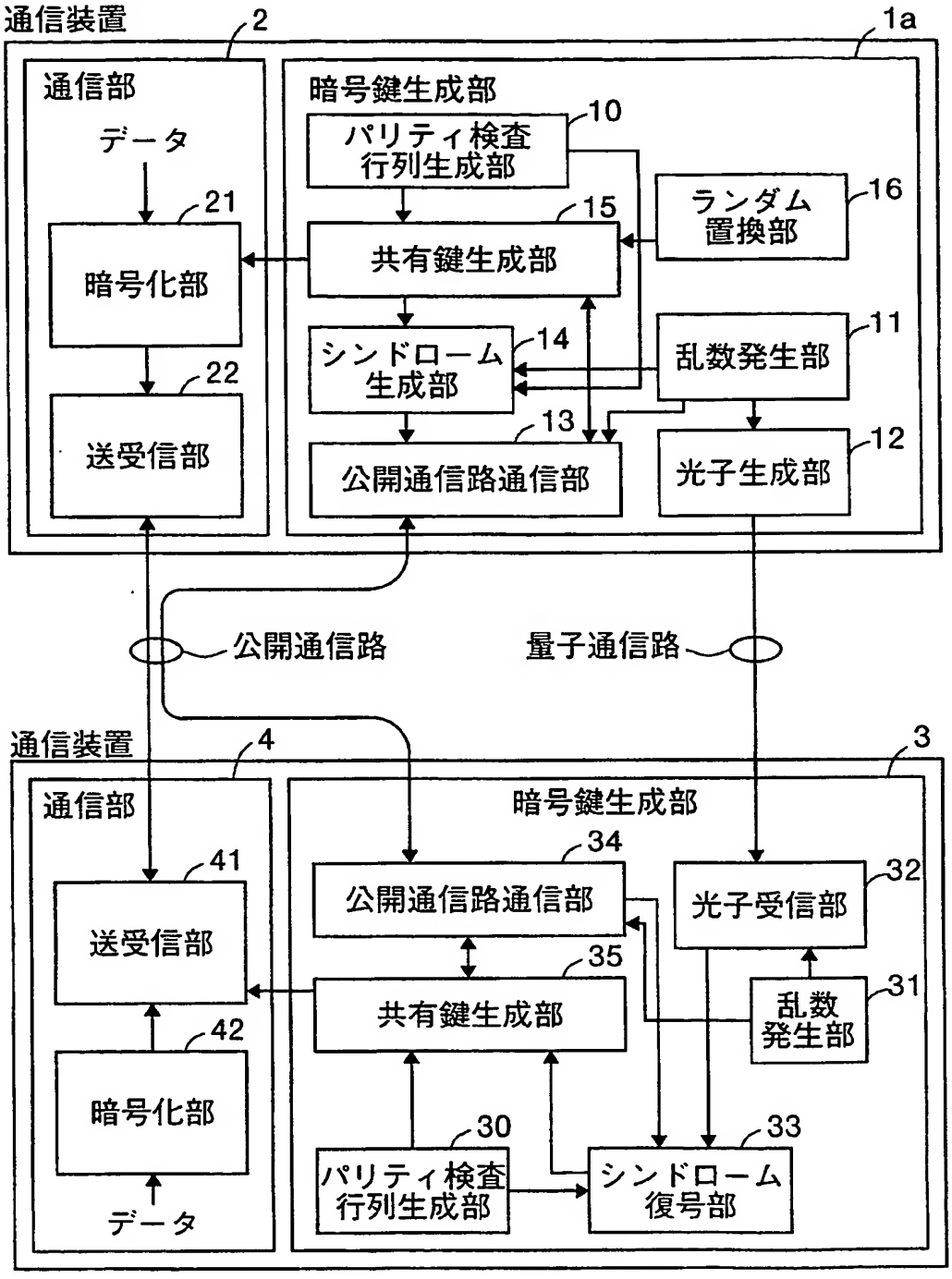
【図５】

rate		0.5	
N		12.6	
i	γ_i	$\lambda(\gamma_i)$	$n(\gamma_i)$
1	2	0.27381	69
2	3	0.10714	18
3	8	0.61905	39
μ		ρ_μ	n_μ
8		1	63

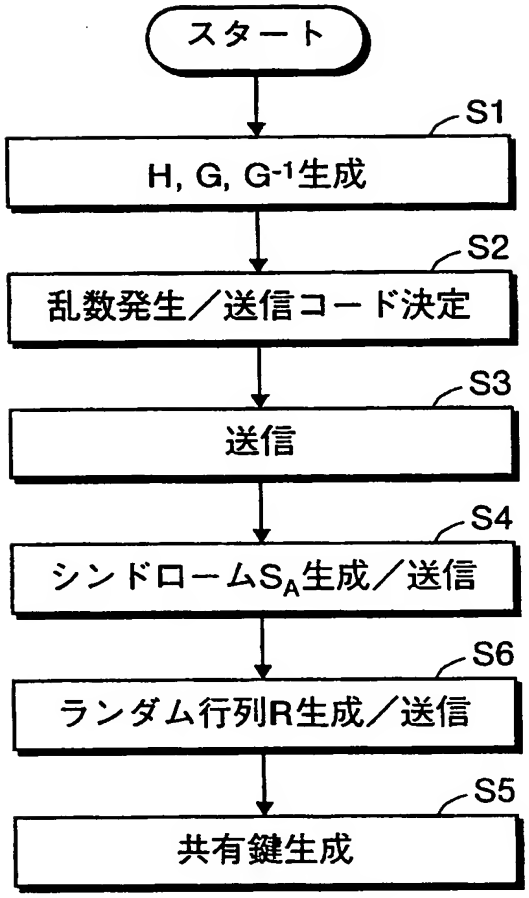
【図６】


BASIC RANDOM SEQUENCE
PERMUTATION PATTURN OF BASIC RANDOM SEQUENCE
C(1) 1
C(2) 2
C(3) 4
C(4) 8
C(5) 5
C(6) 7
C(7) 3
C(8) 6
1 2 3 4 5 6 7 8
LBj(1) 1 2 3 4 5 6 7 8
LBj(2) 2 4 6 8 4 1 3 5
LBj(3) 3 6 1 1 3 7 6 2
LBj(4) 4 8 4 5 8 2 2 7
LBj(5) 5 1 7 2 2 8 5 4
LBj(6) 6 3 2 6 7 3 1 1
LBj(7) 7 5 5 3 1 4 8 6
LBj(8) 8 7 8 7 6 5 4 3
j=1
1 2 3 4 5 6 7 8
Lj,q(1) 1 2 4 8 5 7 3 6
Lj,q(2) 2 4 8 5 7 3 6 1
Lj,q(3) 4 8 5 7 3 6 1 2
Lj,q(4) 8 5 7 3 6 1 2 4
Lj,q(5) 5 7 3 6 1 2 4 8
Lj,q(6) 7 3 6 1 2 4 8 5
Lj,q(7) 3 6 1 2 4 8 5 7
Lj,q(8) 6 1 2 4 8 5 7 3
j=2
1 2 3 4 5 6 7 8
Lj,q(1) 2 8 7 6 1 4 5 3
Lj,q(2) 8 7 6 1 4 5 3 2
Lj,q(3) 7 6 1 4 5 3 2 8
Lj,q(4) 6 1 4 5 3 2 8 7
Lj,q(5) 1 4 5 3 2 8 7 6
Lj,q(6) 4 5 3 2 8 7 6 1
Lj,q(7) 5 3 2 8 7 6 1 4
Lj,q(8) 3 2 8 7 6 1 4 5

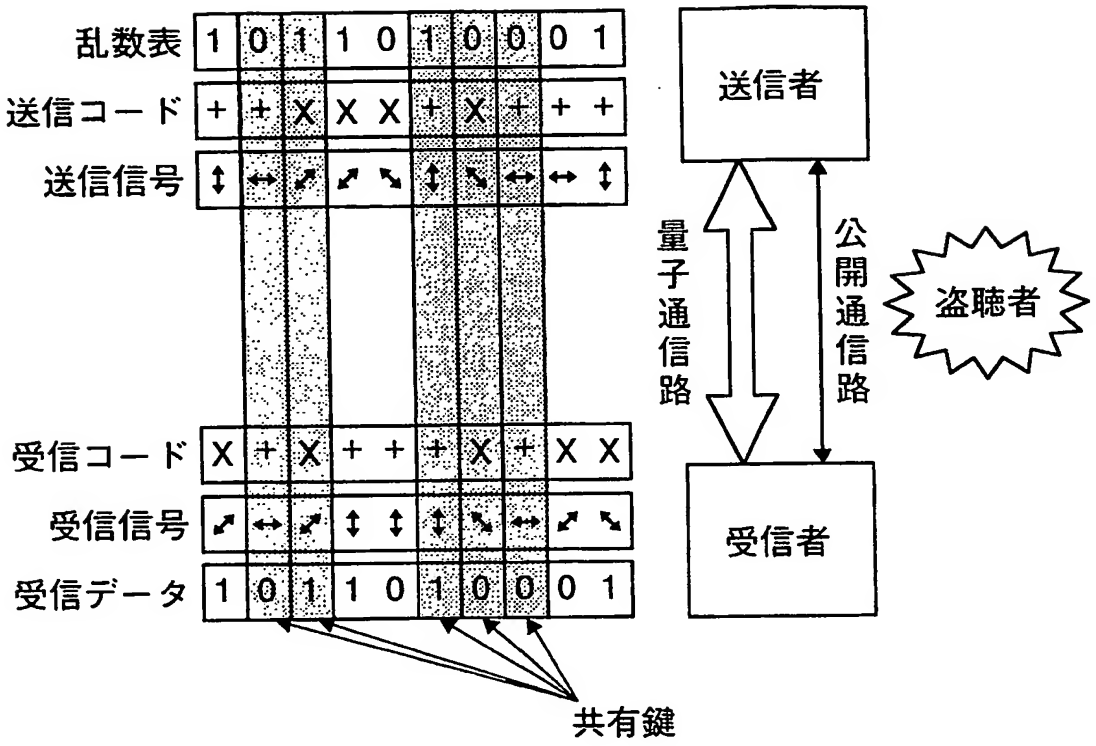
【図７】


通信装置
2
1a
通信部
データ
21
暗号化部
22
送受信部
暗号鍵生成部
10
パリティ検査
行列生成部
15
共有鍵生成部
16
ランダム
置換部
14
シンドローム
生成部
11
乱数発生部
13
公開通信路通信部
12
光子生成部
公開通信路
量子通信路
通信装置
4
3
通信部
41
送受信部
42
暗号化部
データ
暗号鍵生成部
34
公開通信路通信部
32
光子受信部
35
共有鍵生成部
31
乱数
発生部
30
パリティ検査
行列生成部
33
シンドローム
復号部

【図８】


スタート
S1
H, G, G-1生成
S2
乱数発生／送信コード決定
S3
送信
S4
シンドロームSA生成／送信
S6
ランダム行列R生成／送信
S5
共有鍵生成

【図９】


乱数表
1 0 1 1 0 1 0 0 0 1
送信コード
+ + X X X + X + + +
送信信号
受信コード
X + X + + + X + X X
受信信号
受信データ
1 0 1 1 0 1 0 0 0 1
共有鍵
送信者
受信者
量子通信路
公開通信路
盗聴者

【書類名】　要約書

【要約】

【課題】　極めて高い特性を持つ誤り訂正符号を用いて伝送路上におけるデータ誤りを訂正しつつ、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法を得ること。

【解決手段】　本発明の量子鍵配送方法では、受信側の通信装置が、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用のパリティ検査行列を用いて受信データのデータ誤りを訂正し、受信側の通信装置および送信側の通信装置が、公開された誤り訂正情報に応じて共有情報の一部を捨てることとした。

【選択図】　図１

特願２００２－２７１４７３

出　願　人　履　歴　情　報

識別番号　　［０００００６０１３］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　　新規登録
住　所　　東京都千代田区丸の内２丁目２番３号
氏　名　　三菱電機株式会社

特願２００２－２７１４７３

出願人履歴情報

識別番号　［０００００６７９２］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　埼玉県和光市広沢２番１号
氏　名　理化学研究所